UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/603,636	06/26/2000	Yuichi Futa	NAK1-BL53	3314

21611 7590 04/14/2004

SNELL & WILMER LLP
1920 MAIN STREET
SUITE 1200
IRVINE, CA 92614-7230

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	5

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/603,636	Applicant(s) FUTA, YUICHI	
	Examiner Jung W Kim	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-32 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-32 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 26 June 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-32 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to steps for solving a system of linear equations and it is uncertain what performs each of the claimed steps. Moreover, each of the claimed steps, inter alia, storing, transforming, inverting, solving, can be practiced mentally in conjunction with pen and paper. As such the claimed steps do not define a machine or computer implemented process [see MPEP 2106]. Therefore, the claimed inventions are directed to non-statutory subject matter.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 2, 3, 6, 26, 27 and 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contain subject

matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claims 2 and 26 define the use of a pivotal equation, object equation, a first coefficient group, and a second coefficient group without clearly delineating the type/specification of the equation/group that enables an operational transformation process on the linear equations Ax=b defined in claims 1 and 25. Claims 3 and 27 (see steps (a) and (b)) define the limitations of choosing a nonzero coefficient from the pivotal equation and setting the nonzero coefficient into the first coefficient group, choosing a coefficient from the object equation and setting n + 1 values into the second coefficient group, but does not clearly indicate how the coefficients are chosen nor how the values are set. Claims 6 and 30 define the limitation of taking one nonzero coefficient from each pivotal equation and the object equations (step a, primary calculation process), and choosing a nonzero coefficient from the object equation (step a, transformation subprocesses) without clearly specifying taking/choosing steps to operationally enable the steps in steps (a).

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The invention claims steps for solving a system of linear equations wherein these steps are used in encryption or decryption schemes; however,

the claims omits the essential step of using the steps for solving a system of linear equations in an encryption or decryption scheme.

7. Claims 9-24 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. Claims 9-24 define an inverse computing means for computing the inverse of I using the root and solutions found by the equation solving means but fail to adequately claim the method step of how the root and solutions are used to compute the inverse. This omission renders the claims indefinite for failing to distinctly claim the invention.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Curtis Linear Algebra: An Introductory Approach (hereinafter Curtis) in view of Shamir U.S. Patent No. 5,375,170 (hereinafter Shamir). As per claim 1, Curtis teaches means for solving a system of linear equations Ax=b in n unknowns on a field, where n is a positive integer, A is a coefficient matrix consisting of elements of n rows and n

columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements (see Curtis, pages 92-95), comprising:

a. A triangular transforming means for transforming the coefficient matrix A and constant vector b to generate a coefficient matrix A and constant vector b to generate a coefficient matrix A and constant vector b to generate a coefficient matrix C and a constant vector d for a system of linear equations Cx=d in n unknowns that is equivalent to the system of linear equations Ax=b, the coefficient matrix C consisting of elements of n rows and n columns and the constant vector d consisting of n elements, wherein the coefficient matrix A is triangular transformed into the coefficient matrix C of upper triangular form without diagonal elements of the coefficient matrix A being changed to 1 (see Curitis, page 94, 2nd to last paragraph; page 40). Gaussian elimination is used to form the coefficient matrix C, having rows in echelon form, and the corresponding vector d:

i. (E1 * E2 *... * Em * A) * x = (E1 * E2 *... * Em * b) wherein E1, E2, ... Em are elementary row operations and thus

ii. C*x = d.

b. Diagonal element inverting means for calculating inverses of diagonal elements of the generated coefficient matrix C on the field (see Curtis, page 94-95, Example C). Types 1, 2, and 3 elementary operations are used to form identity matrix I from C and hence the inverse of C:

iii. O1 * O2 * ... * On * C = I wherein O1, O2, ... On are elementary operations wherein

iv. O1 * O2 * ... * On = inverse of C.

c. Equation means for solving the system of linear equations Cx=d using the coefficient matrix C, the constant vector d, and the inverses of the diagonal elements of the coefficient matrix C, to thereby solve the system of linear equations Ax=b: x = O1 * O2 *...* On * E1 * E2 *...* Em * b (see Curtis, page 98, exercise 3).

Although Curtis does not explicitly disclose that the method is used in encryption or decryption schemes, means to solve a system of linear equations Ax=b using Gaussian elimination is a well known implementation in cryptographic devices. As an example, Shamir discloses the use of such a triangular transformation to solve a system of linear expressions (see Shamir, col. 11, lines 15-21). Shamir also discloses that finite fields of the type GF(p) are standard fields used in cryptographic algorithms to devise cryptographically secure methods (see Shamir, col. 1, lines 45-48). It would be obvious to one of ordinary skill in the art at the time the invention was made to use Gauss elimination on cryptographic methods which require a solution to the expression Ax=b, since it is standard mathematical means to derive a basis and eventually an inverse to solve for x as taught by Curtis. Finally, an apparatus implementing this transforming means would necessarily have a parameter storing means for storing the matrix A and vector b and a reading means for reading the matrix A and vector b. The aforementioned covers claim 1.

10. As per claim 25, it is a method claim corresponding to claim 1 and it does not teach or define above the information claimed in claim 1. Therefore, claim 25 is rejected as being unpatentable over Curtis in view of Shamir for the same reasons set forth in the rejection of claim 1.

11. As per claims 2-24 and 26-32, the dependent claims are not rejected over the prior art; however, it is unclear whether they are allowable pending clarification of the 35 U.S.C. 101 and 112 issues listed above.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Brandstrom U.S. Patent No. 4,322,577.

Hill "Cryptography in an algebraic alphabet".

Hill "Concerning certain linear transformation apparatus of cryptography".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
March 31, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100